IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

FIRST DATA MERCHANT SERVICES CORPORATION, *et al.*,	*	
Plaintiffs,	*	
v.	*	Civil Action No. RDB-12-2568
SECURITYMETRICS, INC.,	*	
Defendant.	*	

* * * * * * * * * * * * *

MEMORANDUM OPINION

The origins of this contentious case lie in a soured business relationship and the settlement of earlier litigation in the United States District Court for the District of Utah. In this action, Plaintiffs First Data Merchant Services Corporation ("FDMS") and First Data Corporation ("FDC") (collectively "First Data") assert claims against Defendant SecurityMetrics, Inc. ("SecurityMetrics") relating to SecurityMetrics' alleged post-settlement misconduct.[1] SecurityMetrics subsequently asserted fifteen counterclaims sounding in

[1] Specifically, FDMS's original Complaint alleged tortious interference with existing and prospective contractual and business relationships (Count 1), false endorsement/association in violation of the Lanham Act, 15 U.S.C. § 1125(a)(1)(A) (Count 2), trademark, service mark and trademark infringement in violation of the Lanham Act, 15 U.S.C. §§ 1114(1) and 1125(a)(1)(A) (Count 3), false advertising in violation of the Lanham Act 15 U.S.C. § 1125 (a)(1)(b) (Count 4) and common law unfair competition (Count 5). Following a stay of this action pending final disposition of the earlier case filed in the District of Utah and the subsequent denial of FDMS's Preliminary Injunction Motion filed in this Court, FDMS was permitted to amend its Complaint (ECF No. 91).

The Amended Complaint (ECF No. 92) filed by both First Data Plaintiffs seeks declaratory relief (Counts 1 & 9) and alleges breach of contract (Count 2), common law unfair competition (Count 3), tortious interference with existing and prospective contractual and business relationships (Count 4), injurious falsehood (Count 5), as well as violations of the Lanham Act, 15 U.S.C. §§ 1114(1) and 1125(a)(1)(A) (Counts

various doctrines of contract, trademark, and antitrust law. Currently pending before this Court are First Data's Motion for Summary Judgment as to Certain of SecurityMetrics' Counterclaims (ECF No. 272), SecurityMetrics' Motion for Partial Summary Judgment on Contract Claims and Counterclaims (ECF No. 275), First Data's Cross-Motion for Summary Judgment as to First Counterclaim (ECF No. 294), and SecurityMetrics' Motion for Partial Summary Judgment on Common Law Tort and Lanham Act Claims (Counts III-VIII) (ECF No. 277). The parties' submissions have been reviewed, and a hearing was held on December 12, 2014. For the reasons that follow, First Data's Motion for Summary Judgment as to Certain of SecurityMetrics' Counterclaims (ECF No. 272) is GRANTED. SecurityMetrics' Motion for Partial Summary Judgment on Contract Claims and Counterclaims (ECF No. 275) is DENIED and First Data's Cross-Motion for Summary Judgment as to First Counterclaim (ECF No. 294) is GRANTED. Additionally, SecurityMetrics' Motion for Partial Summary Judgment on Common Law Tort and Lanham Act Claims (Counts III-VIII) (ECF No. 277) is DENIED AS MOOT with respect to First Data's Lanham Act claims and DENIED with respect to First Data's tortious interference claim.[2]

Accordingly, the parties are now primed for trial,[3] which is scheduled to begin January 12, 2015. With respect to First Data's claims, the following counts remain:

6, 7, & 8).

[2] At the December 12, 2014 hearing, First Data withdrew its other common law tort claims for unfair competition and injurious falsehoods.

[3] After having resolving the motions for summary judgment, this Memorandum Opinion also addresses a few

declaratory relief (Counts 1 & 9), breach of contract (Count 2), and tortious interference (Count 4). With respect to SecurityMetrics' counterclaims, the following counts remain: declaratory judgment with respect to the third paragraph of the Terms of Settlement (Count 2), and declaratory judgment with respect to the fifth paragraph of the Terms of Settlement (Count 3).

BACKGROUND

In ruling on a motion for summary judgment, this Court reviews the facts and all reasonable inferences in the light most favorable to the nonmoving party. *Scott v. Harris*, 550 U.S. 372, 378 (2007); *see also Hardwick ex rel. Hardwick v. Heyward*, 711 F.3d 426, 433 (4th Cir. 2013).

A. The Payment Card Industry

In the payment card industry, there are a few main types of service providers. An "issuer" issues a payment card to a consumer and bills and collects amounts due from the consumer. The other main service is provided on the merchant side; when a consumer attempts to pay a merchant for goods or services with a payment card, an "acquirer" obtains authorization for the transaction from the consumer's issuer and then clears and settles the transaction so that the merchant gets paid and the consumer's account gets charged.

---

outstanding evidentiary issues. Specifically, SecurityMetrics' request for clarification and/or reconsideration (ECF No. 321) is DENIED AS MOOT. First Data's Motion to Strike the November 12, 2014 'Pinch-Hitting' Declaration of Expert Robert J. Philbin (ECF No. 310) was denied for the reasons indicated on the record at the December 12, 2014 hearing. SecurityMetrics' Motion *in Limine* to Exclude Portions of Expert Report and Testimony of J. Gregory Sidak (ECF No. 296) is DENIED AS MOOT. Finally, SecurityMetrics' Motion *in Limine* to Exclude Portions of Dr. Richard Gering's Report, Testimony, and Demonstrative Exhibits (ECF No. 300) is GRANTED AS MOOT.

Acquirers perform the underwriting requirements and take on the financial risks of fraud. In addition, some payment card brands or associations operate in open networks that allow separate entities or banks to operate as issuers and acquirers; in such open networks, "processors" help to facilitate the communication and settlement of payment. FDMS is an acquirer, while FDC is the payment processor for FDMS's transactions. First Data asserts that it processes transactions for over two million "Level 4" merchants,[4] while SecurityMetrics asserts that the number is closer to 2.6 million. In some cases, pursuant to a contract, First Data stands in the shoes of other acquirers and deals with the acquirers' merchants directly; in those cases, First Data undertakes the underwriting and risk management responsibilities and is liable for losses or fines incurred by the Acquirer. First Data performs acquirer services from approximately 820,000.

The term "PCI" is as an acronym for "Payment Card Industry." The PCI Security Standards Council ("PCI Council") was formed in 2006 by the major credit card brands. The PCI Council developed the PCI Data Security Standard ("PCI Standard" or "PCI DSS"), which has been adopted by the major credit card brands as their data security compliance requirement for all merchants. Thus, the card brands enforce compliance with the PCI Standard and determine the penalties for non-compliance. While the PCI Standard's requirements vary based upon the size of a merchant, the category of merchants

[4] Within the payment card industry, merchants are categorized based upon the volume of their transactions. Level 4 merchants have the lowest transaction volume and are the category of merchants at issue in this case.

at issue in this case are "Level 4 merchants."[5] Level 4 merchants are more numerous than higher-volume merchants and, as such, have the highest number of transactions collectively.

While the PCI standard is universal, the various Card Brands have different requirements for demonstrating or validating compliance with the standard. The category at issue in this case are "Level 4 merchants"[6]—those merchants with the lowest transaction volume. Level 4 merchants are more numerous than higher-volume merchants and, as such, have the most collective transactions. For these lower-volume merchants, the PCI Council provides the Self-Assessment Questionnaire ("SAQ"). The SAQ is a validation tool intended to assist merchants in self-evaluating their compliance with the PCI Standard. For those Level 4 merchants who conduct sales over the internet, however, the PCI Data Security Standard requires vulnerability scans of its computer system. These scans must be performed by Approved Scanning Vendors ("ASV"), which are approved by the PCI Council. SecurityMetrics is certified by the PCI Council as an ASV, but First Data is not.[7]

---

[5] Specifically, SecurityMetrics alleges:

> For PCI Standard compliance validation purposes, Visa, MasterCard, and Discover each divide merchants into four levels; American Express divides them into three; and JCB divides them into two. Following the classifications used by Visa and MasterCard, the lowest-volume merchants are commonly referred to as "Level 4 merchants."

Def.'s Countercl. ¶ 30. The Court adopts this terminology herein.

[6] Specifically, SecurityMetrics alleges:

> For PCI Standard compliance validation purposes, Visa, MasterCard, and Discover each divide merchants into four levels; American Express divides them into three; and JCB divides them into two. Following the classifications used by Visa and MasterCard, the lowest-volume merchants are commonly referred to as "Level 4 merchants."

Def.'s Countercl. ¶ 30. The Court adopts this terminology herein.

[7] SecurityMetrics also has several additional certifications that First Data does not, including certifications as a Qualified Security Assessor ("QSA"), Payment Application Qualified Security Assessor ("PA-QSA"), PCI

B. The Relationship of the Parties

First Data is a global payment processor engaged in the business of processing credit and debit card transactions for merchants and independent sales organizations ("ISOs") who use First Data's card processing services. SecurityMetrics provided compliance services to some merchants for whom First Data provides processing services. For those merchants that First Data provides acquirer services (some 820,000 merchants), First Data has instituted a PCI Standard compliance reporting program.

For several years, the parties worked together pursuant to a series of contracts.[8] Under those agreements, "First Data promoted SecurityMetrics to its Level 4 merchant customers as its preferred vendor for services relating to validation of compliance with PCI Standards, and SecurityMetrics developed and utilized a protocol for reporting validation of compliance through what is known as the "START" system. START is not an industry standard and it is not prescribed by the PCI Council." Under the terms of the agreement, First Data paid SecurityMetrics for each merchant that was enrolled (usually for a 1 year service period), and SecurityMetrics would report the compliance status of all its enrolled merchants to First Data on a monthly basis. The agreement was last renewed on January 3, 2012. SecurityMetrics alleges, however, that First Data materially breached the agreement in

---

Forensic Investigator ("PFIs"), and Point-to-Point Encryption assessors ("P2PE").

[8] For purposes of this Memorandum Opinion, the relevant documents include the original January 2008 contract (the "Master Services Agreement") (ECF No. 275-2) and a separate "Statement of Work" (ECF No. 275-3), and the 2011 Amendment to the Master Services Agreement (ECF No. 275-5).

April 2012 and then unilaterally and prematurely terminated it in May 2012.[9] Since that point, SecurityMetrics ceased SMART reporting and began to send emails containing links to PDF reports of compliance.

In June of 2012, First Data began offering a service called "PCI Rapid Comply," which competes with the services offered by SecurityMetrics.[10] First Data asserts that PCI Rapid Comply is only available to those Level 4 merchants for whom First Data supplies acquirer services—some 820,000 merchants. First Data also alleges that only 200,000 merchants have actually used PCI Rapid Comply to report their PCI Standard compliance.

SecurityMetrics alleges various unfair practices on First Data's part in connection to the roll-out of PCI Rapid Comply. First Data imposes billing minimums on ISOs using First Data for acquirer services, and SecurityMetrics alleges that, when calculating these minimums, First Data counts fees for PCI Rapid Comply towards the required minimums, but refuses to count costs or fees paid to vendors of other PCI compliance services. In addition, SecurityMetrics asserts that First Data represented that merchants who used compliance verification vendors other than PCI Rapid Comply would have to pay for those services in addition to the cost of PCI Rapid Comply.

---

[9] Accordingly to First Data, the event that precipitated the falling-out was First Data's instruction to SecurityMetrics to stop using the data provided by First Data for out-bound solicitations to Level 4 merchants. First Data believes that this action was consistent with the contract. First Data alleges that, thereafter, SecurityMetrics accused First Data of breaching the contract, cut off First Data's access to SecurityMetrics' interactive database, and stopped submitting PCI compliance reports with the START feeds.

[10] As noted *infra*, this service is now being wound down.

In May of 2012, FDMS filed suit in *First Data Merchant Services Corporation v. SecurityMetrics, Inc.*, Case No. 2:12-cv-495 ("Utah Action") in the United States District Court for the District of Utah ("Utah Court") and moved for a temporary restraining order and preliminary injunction requiring SecurityMetrics to resume START reporting. The Utah Court denied the motion, and the parties entered mediation, which resulted in the signing of Terms of Settlement ("Settlement Terms") by both parties. Under those terms, First Data proffered a payment of five million dollars.

C. The Presently Pending Action

On August 27, 2012—less than three months after the signing of the Terms of Settlement—First Data filed the presently pending action before this Court. Following a stay of this action pending final disposition of the Utah Action and the subsequent denial of FDMS's Preliminary Injunction Motion filed before this Court, FDMS was permitted to amend its Complaint (ECF No. 91). As a result, First Data filed the Amended Complaint (ECF No. 92) on March 8, 2013, which asserted the following claims:

1) Declaratory relief (Count 1)
2) Breach of contract (Count 2)
3) Common Law Unfair Competition (Count 3)
4) Tortious Interference with Existing and Prospective Contractual and Business Relationships (Count 4)
5) Injurious Falsehoods (Count 5)

6) False Endorsement/Association, Lanham Act 15 U.S.C. § 1125(a)(1)(A) (Count 6)
7) Trademark/Service Mark/Trade Name Infringement, Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A) (Count 7)
8) False Advertising, Lanham Act, 15 U.S.C. 1125(a)(1)(B) (Count 8)
9) Declaratory Relief (Count 9)

SecurityMetrics answered the Complaint on August 26, 2013 and asserted fifteen counterclaims of its own against First Data, including claims for:

1) Specific performance of the first paragraph of the Terms of Settlement (Obligation to Enter Long-Form Settlement) (Count 1)
2) Declaratory judgment with respect to third paragraph of the Terms of Settlement (Merchant Data provision) (Count 2)
3) Declaratory judgment with respect to fifth paragraph of the Terms of Settlement (Unenforceability of Confidentiality Term) (Count 3)
4) Injurious falsehoods (Count 4),
5) Federal false advertising (Count 5),
6) Federal false endorsement (Count 6),
7) Cancellation of registration (Count 7),
8) Utah Deceptive Trade Practices violations (Count 8),
9) Tortious interference (Count 9),
10) Federal restraint of trade (Count 10),

11) Federal monopolization and attempted monopolization (Count 11),

12) Maryland Restraint of Trade (Count 12)

13) Maryland monopolization and attempted monopolization (Count 13)

14) Maryland predatory pricing (Count 14), and

15) Maryland tying (Count 15).

First Data's Motion to Dismiss Certain of Defendant's Counterclaims (ECF No. 163), filed on September 19, 2013, targeted only a few of these counts. That Motion was denied with the exception of SecurityMetrics' attempt to assert monopolization claims in Counts Eleven and Thirteen. (The attempted monopolization claims, however, were permitted to proceed).

D. Recent Developments

Since the initiation of this lawsuit, First Data has apparently decided to wind down its PCI Rapid Comply service. Specifically, on June 11, 2014, First Data announced a new partnership with Trustwave, a third-party PCI compliance vendor. According to First Data, "PCI Rapid Comply will be taken over and powered by Trustwave, and Trustwave will essentially be the new preferred PCI compliance vendor that [SecurityMetrics] used to be." Mem. Supp. Mot. Summ. J. Certain Countercls. at 12, ECF No. 273.

STANDARD OF REVIEW

Rule 56 of the Federal Rules of Civil Procedure provides that a court "shall grant summary judgment if the movant shows that there is no genuine dispute as to any material

fact and the movant is entitled to judgment as a matter of law." FED. R. CIV. P. 56(c). A material fact is one that "might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). A genuine issue over a material fact exists "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Id.* When considering a motion for summary judgment, a judge's function is limited to determining whether sufficient evidence exists on a claimed factual dispute to warrant submission of the matter to a jury for resolution at trial. *Id.* at 249.

In undertaking this inquiry, this Court must consider the facts and all reasonable inferences in the light most favorable to the nonmoving party. *Scott v. Harris*, 550 U.S. 372, 378 (2007). However, this Court must also abide by its affirmative obligation to prevent factually unsupported claims and defenses from going to trial. *Drewitt v. Pratt*, 999 F.2d 774, 778-79 (4th Cir. 1993). If the evidence presented by the nonmoving party is merely colorable, or is not significantly probative, summary judgment must be granted. *Anderson*, 477 U.S. at 249-50. On the other hand, a party opposing summary judgment must "do more than simply show that there is some metaphysical doubt as to the material facts." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986); *see also In re Apex Express Corp.*, 190 F.3d 624, 633 (4th Cir. 1999). This Court has previously explained that a "party cannot create a genuine dispute of material fact through mere speculation or compilation of inferences." *Shin v. Shalala,* 166 F. Supp. 2d 373, 375 (D. Md. 2001) (citations omitted).

When both parties file motions for summary judgment, as here, the court applies the same standard of review to both motions, with this Court considering "each motion

separately on its own merits to determine whether either [side] deserves judgment as a matter of law." *Rossignol v. Voorhaar*, 316 F.3d 516, 523 (4th Cir. 2003), *cert denied*, 540 U.S. 822 (2003); *see also havePower, LLC v. Gen. Elec. Co.*, 256 F. Supp. 2d 402, 406 (D. Md. 2003) (citing 10A Charles A. Wright & Arthur R. Miller, *Federal Practice & Procedure* § 2720 (3d ed. 1983)).

ANALYSIS

The parties' motions for summary judgment break the various claims and counterclaims in this action into several different broad categories. SecurityMetrics' Motion for Partial Summary Judgment on Contract Claims and Counterclaims (ECF No. 275) and First Data's Cross-Motion for Summary Judgment as to the First Counterclaim both address the claims raised by both parties concerning the interpretation and effect of the Terms of Settlement. SecurityMetrics' Motion for Partial Summary Judgment on Common Law Tort and Lanham Act Claims (Counts III-VIII) (ECF No. 277) addresses First Data's claims involving SecurityMetrics' advertising and marketing practices. SecurityMetrics asserts similar claims based upon First Data's marketing, and First Data has moved for judgment on those counterclaims in its Motion for Summary Judgment as to Certain of SecurityMetrics' Counterclaims (ECF No. 272). Additionally, that motion also addresses SecurityMetrics' antitrust counterclaims. This Court will address the issues raised by the parties' papers in the order outlined above.

I. SecurityMetrics' Motion for Partial Summary Judgment on Contract Claims and Counterclaims (ECF No. 275)

SecurityMetrics' first Motion for Partial Summary Judgment pertains to Counts 1 and 2 of First Data's Amended Complaint (ECF No. 92) and Count 1 and part of Count 2 of SecurityMetrics' Counterclaims.[11] The two main issues raised by the Motion concern the legal effect of the Terms of Settlement—specifically, (A) the scope of SecurityMetrics' right to use information about First Data's merchants for marketing purposes, and (B) SecurityMetrics' right to an order forcing First Data to sign and comply with a June 11, 2012 long-form settlement draft proposed by First Data.

A. Interpretation of the "Merchant Data" Provision

The first issue pertains to the "Merchant Data Provision" of the Terms of Settlement, which states that SecurityMetrics "may make any use of Merchant Data for the purpose of selling its products and services, but may not sell any such data to a third-party (other than the sale of SM to a third party)." Both parties agree that the term "Merchant Data" in the Terms of Settlement is governed by the definition of that term in the parties' previous contracts. The original January 2008 contract (the "Master Services Agreement") included the following definitions:

> "Merchants" means FDMS' payment processing merchants or vendors for which SecurityMetrics will provide security services as outlined in any Statement of Work.
>
> "Merchant Data" means information and data relating to Merchants and their computer and security systems.

[11] SecurityMetrics also suggests that granting this motion would have the effect of mooting Count 9 of First Data's Amended Complaint.

Additionally, a 2011 Amendment to the original contract modified the definition of the term merchants accordingly:

> "Merchants" means payment processing merchants or vendors whose contact information has been loaded into the FDIS or FDMS merchant compliance console for which SecurityMetrics will provide security services as outlined in any Statement of Work.

The issue before the Court is whether the Merchant Data provision—and the incorporated definitions from the parties' contracts—granted SecurityMetrics the right to use the data for only those merchants who had enrolled in its services ("Enrolled Merchants") or for any merchant for which SecurityMetrics received information during the parties' relationship under the contract. At the motion to dismiss stage, this Court ruled that the Merchant Data provision was ambiguous.[12]

[12] Specifically, this Court ruled that:

> According to First Data, the phrase "for which SecurityMetrics will provide services as outlined in any Statement of Work" signifies that "SecurityMetrics is precluded post-termination from using data about Unenrolled Merchants that it previously received from FDMS to market PCI compliance services to those merchants." Pls.' Opp. to Def.'s Mot. to Dismiss at 10, ECF No. 115. On its end, SecurityMetrics argues that "provide" means "to supply or make available." Def.'s Reply to Pls.' Opp. at 7, ECF No. 122. Specifically, SecurityMetrics contends that while it *supplied* services to Enrolled Merchants, it *made its services available* to Unenrolled Merchants. *Id.* As stated above, when "the language of the agreement is reasonably susceptible to [either parties'] contended interpretation, . . . [the agreement] is ambiguous, and any evidence relevant to prove its meaning is admissible." *Ward*, 907 P.2d at 269. In this case, as "the contrary positions of the parties [are] each . . . tenable," *Uintah Basin Med. Ctr.*, 2005 UT App. 92 at ¶ 13, the provision relating to SecurityMetrics' use of Merchant Data in the Terms of Settlement is ambiguous. As such, "extrinsic evidence must be looked to in order to determine the intentions of the parties." *Dixon v. Pro Image Inc.*, 1999 UT 89, ¶ 14, 987 P.2d 48. Extrinsic evidence regarding the meaning of "Merchant" is not presently before the Court. Moreover, it is well

In its Motion for Partial Summary Judgment, SecurityMetrics argues that, when read in context, the Merchant Data provision is not ambiguous. In support of this position, SecurityMetrics points to the additional definitions added by the 2011 Amendment, which included the terms "Refused,"[13] "Enrolled,"[14] and "No Response."[15] These definitions, in SecurityMetrics' view, indicate that "Enrolled Merchants" are a subset of "Merchants." SecurityMetrics asserts that its reading of the contract gives meaning to these terms and First Data's reading (i.e., excluding unenrolled merchants from the definition of "Merchants") would render those additional terms a contractual nullity. SecurityMetrics also points to additional modifications from the 2011 Amendment (the first—paragraph 2 of the 2011 Amendment—stating that "all registered Merchant profiles regardless of status are to remain available for enrollment or re-enrollment" during the contract term, and the other—Section

---

> established that "the construction of ambiguous provisions is a factual determination that precludes dismissal on a motion for failure to state a claim." *Martin Marietta Corp. v. Int'l Telecomm. Satellite Org.*, 991 F.2d 94, 97 (4th Cir. 1992); *see also Kreisler & Kreisler, LLC v. Nat'l City Bank*, 657 F.3d 729, 731 (8th Cir. 2011) ("If the language is susceptible to more than one meaning, then resolution of the ambiguity as to the parties' intent is a question of fact and the court should not grant a motion to dismiss."); *Eternity Global Master Fund Ltd. v. Morgan Guar. Trust Co. of N.Y.*, 375 F.3d 168, 178 (2d Cir. 2004) ("[A] claim predicated on a materially ambiguous contract term is not dismissible on the pleadings."); *Dawson v. Gen. Motors Corp.*, 977 F.2d 369, 373 (7th Cir. 1992) (same proposition). Accordingly, Defendant SecurityMetrics' Motion to Dismiss Counts I and II of Plaintiffs' Amended Complaint is DENIED.

Mem. Op. Mot. Dismiss Am. Compl. 11-12, ECF No. 152.

[13] "Refused" means a Merchant that has refused the Services after having been contacted by SecurityMetrics.

[14] "Enrolled" means a Merchant that is currently enrolled to receive SecurityMetrics Services.

[15] "No Response" means a Merchant that, after repeated attempts by SecurityMetrics to contact, has not responded to any such communication efforts.

11.2.1—stating that "no new Merchants may enroll for Services" after the termination of the contract term) as further support for its position. Alternatively, SecurityMetrics argues that it is entitled a summary judgment ruling in its favor because, in its view, First Data has failed to present sufficient extrinsic evidence to generate a question of material fact.

In response, First Data argues that summary judgment should be denied because the Terms of Settlement are ambiguous and, therefore, the trier of fact must assess the extrinsic evidence. First Data argues that the express definition of merchant includes the phrase "for which SM will provide security services," meaning that a Merchant must, by the term's definition, be enrolled in SecurityMetrics' services.[16]

The parties agree that Utah law governs the contractual claims and the interpretation of the Terms of Settlement. The Utah Supreme Court has articulated the following principles for courts to apply in interpreting contractual language:

> In interpreting a contract, the intentions of the parties are controlling. *Dixon v. Pro Image, Inc.*, 1999 UT 89, ¶ 13, 987 P.2d 48 (quotation omitted). "[W]e first look to the four corners of the agreement to determine the intentions of the parties. *Ron Case Roofing & Asphalt v. Blomquist*, 773 P.2d 1382, 1385 (Utah 1989); *see also Reed v. Davis Co. Sch. Dist.*, 892 P.2d 1063, 1064–1065 (Utah Ct. App. 1995). If the language within the four corners of the contract is unambiguous, the parties' intentions are determined from the plain meaning of the contractual language, and the contract may be interpreted as a matter of law. *Dixon,* 1999 UT 89 at ¶ 14, 987 P.2d 48 (citing *Willard Pease Oil & Gas Co. v. Pioneer Oil & Gas Co.*, 899 P.2d 766, 770 (Utah 1995)). If the language within the four corners of the contract is ambiguous, however, extrinsic evidence must be looked to in order to determine the intentions of the parties. *Id.* In evaluating whether the plain

[16] First Data also rejects SecurityMetrics' reliance upon other provisions in the parties' earlier agreement. In First Data's view, Section 11.3.1 means merely that SecurityMetrics will not enroll new merchants after the termination of the contract. Similarly, it asserts that paragraph 2 of the 2011 Amendment merely dealt with the re-enrollment or recertification of merchants, which was the purpose of the amendment.

> language is ambiguous, we attempt to harmonize all of the contract's provisions and all of its terms. *Id.*; *see also Buehner Block Co. v. UWC Assocs.*, 752 P.2d 892, 895 (Utah 1988). "An ambiguity exists where the language 'is reasonably capable of being understood in more than one sense.' " *Dixon*, 1999 UT 89 at ¶ 14, 987 P.2d 48 (quoting *R & R Energies v. Mother Earth Indus., Inc.*, 936 P.2d 1068, 1074 (Utah 1997) (further quotation omitted)).

Central Fla. Invs. v. Parkwest Assocs., 2002 UT 3, ¶ 12, 40 P.3d 599.

The Court of Appeals of Utah has held that "[t]o demonstrate ambiguity, the contrary positions of the parties must each be tenable." *Uintah Basin Med. Ctr. v. Hardy*, 2005 UT App. 92, ¶ 13, 110 P.3d 168. As such, the Supreme Court of Utah has held that if "the language of the agreement is reasonably susceptible to [either parties'] contended interpretation, . . . [the agreement] is ambiguous, and any evidence relevant to prove its meaning is admissible." *Ward v. Intermountain Farmers Ass'n*, 907 P.2d 264, 269 (Utah 1995) (citation omitted). However, it has also held that "words and phrases do not qualify as ambiguous simply because one party seeks to endow them with a different interpretation according to his or her own interests." *Saleh v. Farmers Ins. Exch.*, 2006 UT 20, ¶ 17, 133 P.3d 428 (citing *Alf v. State Farm Fire & Cas. Co.*, 850 P.2d 1272, 1274-75 (Utah 1993)). Finally, in Utah, it is "the rule of law that where two or more instruments are executed by the same parties . . . in the course of the same transaction, and concern the same subject matter, they will be read and construed together so far as determining the respective rights and interests of the parties." *Bullfrog Marina, Inc. v. Lentz*, 501 P.2d 266, 271 (Utah 1972).

As noted above, this Court has already determined that the Merchant Data provision is ambiguous. *See* MTD Am. Compl. 11-12. The specific contractual definitions limit the

scope of "Merchants" to those "for which SecurityMetrics will provide services." This phrase is capable of an interpretation that is either limited to only Enrolled Merchants or one that encompasses both Enrolled and Unenrolled Merchants. *See id.* The other clauses in the contract and its amendments identified by SecurityMetrics—particularly those touching upon SecurityMetrics' data rights—are insufficient to purge the ambiguity contained within the definition of one of the main terms of the contract.

In light of this ambiguity, this Court must turn to the extrinsic evidence of intent proffered by the parties. SecurityMetrics argues that the only extrinsic evidence identified by First Data—the deposition testimony of Blaine Benard, an attorney for First Data, and Bradley Caldwell, one of SecurityMetrics' Rule 30(b)(6) deponents on damages—does not provide any support for First Data's positions and, in fact, support its own reading of the contract.[17] Citing to Benard's testimony that there was no discussion of the meaning of the term "Merchant Data" during the negotiations between First Data and SecurityMetrics prior to the execution of the Terms of Settlement, SecurityMetrics argues that Benard's deposition demonstrates that First Data has no parol evidence with respect to the meaning of the contractual language. On the other hand, First Data contends that his testimony is relevant because it reinforces the notion that there was no mutual intent to extend the term

[17] Additionally, SecurityMetrics identifies further extrinsic evidence that it views as supporting its position, including the fact that (1) much of the Merchant Data was not provided by First Data but had been developed by SecurityMetrics; (2) that SecurityMetrics reported on enrolled *and* unenrolled merchants; (3) SecurityMetrics reduced its settlement demand in exchange for the Merchant Data provision in the Terms of Settlement.

"Merchant Data" beyond that in the original contract and that First Data was not aware of any other definition of the term prior to the execution of the Terms of Settlement.

The parties' dispute regarding Caldwell's testimony is of a similar nature. Caldwell testified that it was SecurityMetrics' understanding that the Terms of Settlement permitted SecurityMetrics to use data for all merchants, not just its customers, for marketing its products and services. In opposition, First Data points out that Caldwell stated that SecurityMetrics believed that, under the original contract and its amendments, SecurityMetrics was only allowed to use the data of merchants whom SecurityMetrics had enrolled as a customer. First Data asserts that this is party admission as to the meaning of "Merchant Data." In reply, SecurityMetrics argues that First Data has misconstrued Caldwell's testimony because Caldwell was testifying about the scope of SecurityMetrics' merchant data rights and not the specific definition of "Merchant" or "Merchant Data." SecurityMetrics also points out that the provisions defining the scope of SecurityMetrics' merchant data rights in the prior contract documents included the phrase "who have enrolled with SecurityMetrics prior to the date of termination," but that the Terms of Settlement does not include any such limiting language.

Having reviewed the parties' arguments, this Court finds that both positions are supported by extrinsic evidence. First Data has demonstrated that there were no discussions regarding modifying the meaning of the contractual definitions and that SecurityMetrics understood the original contract to limit its rights with respect to the use of merchant data. SecurityMetrics, however, has offered evidence suggesting that SecurityMetrics lowered its

settlement demand amount after the removal of language limiting its rights with respect to merchant data. Accordingly, the intent of the parties must be determined by the jury at trial, and SecurityMetrics' motion for summary judgment will be denied.

B. Obligation to Execute a "Final Settlement Agreement"

The parties have also filed cross-motions for summary judgment as to the first provision of the Terms of Settlement, which states that "[t]he parties shall incorporate these terms of settlement in a final settlement agreement, in a form and with content mutually acceptable to both parties, which shall be executed in advance of the $5,000,000 payment set forth in these Terms of Settlement." First Data proposed one version of such a long-form settlement on June 11, 2012. SecurityMetrics responded by proposing three changes (which it characterizes as minor).[18] First Data did not agree to those changes and the parties were never able to simultaneously agree to language for a long-form settlement after that point.

In its papers, SecurityMetrics argues that First Data's course of action violated the obligation to finalize a long-form settlement agreement. SecurityMetrics first argues that the Terms of Settlement constitutes an enforceable agreement to agree. Citing to 1-2 CORBIN ON CONTRACTS § 2.8, SecurityMetrics argues that agreements to agree should be honored unless the court is forced to "fill in the gap in the dark." *See* Mem. Supp. MPSJ Contract Cls. & Countercls. 24. SecurityMetrics argues that the June 11 draft enables this Court to enforce the agreement to agree without operating in the dark. Alternatively, SecurityMetrics argues that the obligation to enter into a final settlement made First Data's proposed draft

[18] The first modification addressed a typo, the second sought broader exceptions for the confidentiality provisions; and the third sought to remove a provision from the venue clause.

irrevocable. As an additional alternative, SecurityMetrics suggests that this Court find that "a promise to enter into a final written settlement agreement carries with it . . . an obligation to *negotiate* toward such an agreement *in good faith*," and asserts that First Data's actions indicate that it did not operate in good faith.

In its papers and at the hearing, SecurityMetrics acknowledged that its positions are basically requesting "an extension" of existing law and characterizes the issues before the Court as a matter of "first impression." *See* SecurityMetrics' Reply – Contract Cls. & Countercls. at 18; Mem. Supp. MPSJ Contract Cls. & Countercls. at 26. SecurityMetrics argues that one of its various proposed rules must be applied in order to give effect to the first provision of the Terms of Settlement. The facts of this case, however, do not align neatly with the theories proposed by SecurityMetrics. The Terms of Settlement provision makes no mention of an obligation to negotiate. Furthermore, SecurityMetrics has failed to identify any provision from the June 11, 2012 settlement offer that states (either expressly or implicitly) the offer will remain open or is irrevocable. This lack of fit is only compounded by the fact that SecurityMetrics has failed to identify a single analogous case—whether arising under the law of Utah or any other state;[19] indeed, SecurityMetrics acknowledges that

[19] The only cases identified by SecurityMetrics—and referenced by a "Cf."—are *Murray v. State*, 737 P.2d 1000 (Utah 1987), and *John Deere Co. v. A&H Equip., Inc.*, 876 P.2d 880, 883 (Utah App. 1994). In *Murray*, the defendant made an initial written offer of settlement. During a later phone call, plaintiff's counsel indicated that the plaintiff had accepted the offer and the defendant tendered a check. Several days later, the plaintiff changed her mind, refused the sign the settlement, and returned the check. As this summary should make clear, *Murray* is inapposite because in that case an acceptance preceded a rejection; SecurityMetrics, however, initially rejected the offer and subsequently wished to accept it.

Similarly, in *John Deere Co. v. A&H Equip., Inc.*, the defendant and counterclaimant A&H Equipment, Inc. initially proposed a settlement that would have released the parties' claims against each other. John Deere verbally accepted the settlement and then sent a letter indicating John Deere's acceptance.

its position requires an extension of existing law. Under these circumstances, this Court—sitting in diversity—is unwilling to adopt the new rules proposed by SecurityMetrics.

Accordingly, the Court must rely upon traditional contract principles in analyzing the question of contact formation with respect to a long-form settlement agreement. Under these principles, "a counteroffer operates as a rejection of the original offer" and "[t]he offeree's power to accept the original offer is thereby terminated." *Cea v. Hoffman*, 276 P.3d 1178, 1186 (Utah Ct. App. 2012). It is undisputed that, in this case, counsel for SecurityMetrics countered First Data's June 11, 2012 draft settlement with a demand for three changes. This communication operates as a counteroffer rejecting the June 11 settlement offer and terminating SecurityMetrics' ability to accept the June 11, 2012 settlement draft. Accordingly, SecurityMetrics' motion for partial summary judgment will be denied with respect to the first provision of the Terms of Settlement, and First Data's Cross-Motion for Summary Judgment as to SecurityMetrics' First Counterclaim will be granted.

II. SecurityMetrics' Motion for Partial Summary Judgment on Common Law Tort and Lanham Act Claims (Counts III-VIII)

A. Lanham Act Claims

First Data has asserted claims under the Lanham Act, alleging that various representations by SecurityMetrics constituted false endorsement, false advertising, and/or

---

Subsequently, John Deere began preparing the settlement documents. Upon reviewing those documents, however, A&H refused to sign them because it claimed that it also sought release from a previous judgment entered against it payable to a related but independent third party. Again, in *John Deere*, the court ruled that an acceptance had preceded a subsequent rejection.

trademark infringement.[20] At the December 12, 2014 hearing, the parties discussed the possibility of resolving First Data's Lanham Act claims by a consent order. The parties submitted proposed draft orders and ultimately came to agreement on a Consent Order signed by this Court on December 22, 2014. *See* ECF No. 334. Accordingly, SecurityMetrics' Motion for Partial Summary Judgment is now moot with respect to Counts 6, 7, and 8 of First Data's Amended Complaint, and SecurityMetrics' Motion will therefore be denied as moot with respect to those claims.

B. Common Law Tort Claims

First Data's Amended Complaint included common law tort claims for unfair competition (Count 3), tortious interference (Count 4), and injurious falsehoods (Count 5). At the December 12, 2014 hearing, First Data agreed to withdraw its claims for unfair competition and injurious falsehoods. Accordingly, only the tortious interference claims is currently before this Court.

In order to prevail on a claim for tortious interference, the plaintiff must prove that the defendant "committed 1) intentional and willful acts; 2) calculated to cause damage to plaintiff in its lawful business; 3) done with an unlawful or improper purpose; 4) that results in actual damages." *See Nat'l. Bd. for Certification in Occupational Therapy, Inc. v. Am. Occupational Therapy Ass'n.* (NBCOT), 24 F. Supp. 2d 494, 505-506 (D. Md. 1998).

The main grievance addressed by First Data's tortious interference claim appears to

[20] Additionally, First Data seeks injunctive relief under Count 4 for tortious interference on the basis of these marketing practices.

pertain to the format of SecurityMetrics' PCI compliance reporting.[21] After the termination of the contract, SecurityMetrics abandoned the START system reporting and began to send its compliance reports by individual emails. In order to process the numerous emails received each day, First Data first hired temporary employees to process these emails and subsequently developed a computer program that automatically processed SecurityMetrics' emailed reports. It is these costs that First Data now seeks to recover as damages.

SecurityMetrics denies liability on several grounds.[22] SecurityMetrics' arguments rest upon paragraph 19 of the Statement of Work, which provides that if the Master Services Agreement or Statement of Work were terminated, "compliance charges for weekly data feeds will apply and be mutually determined." SecurityMetrics argues that First Data's failure to pay any such "mutually determined" "compliance charges" constitutes the proximate cause of First Data's claimed injuries. Alternatively, SecurityMetrics suggests that First Data's tortious interference claim fails based on the doctrine of avoidable consequences due to First Data's failure to pay such charges.[23] Finally, SecurityMetrics argues that First Data's

[21] First Data's Amended Complaint also makes reference to SecurityMetrics' marketing practices. *See* Am. Compl. ¶ 214. However, based upon First Data's representations in its papers, at the December 12, 2014 hearing, and the parties' resolution of First Data's Lanham Act claims, it appears to the Court that the only remaining theory of liability with respect to the tortious interference claim *for damages* relates to SecurityMetrics' reporting practices.

[22] These arguments arise in SecurityMetrics Reply brief. *See* Reply 2-7, ECF No. 305. In its opening brief, SecurityMetrics also argued that First Data had failed to identify any relationship with which SecurityMetrics had interfered. The Court does not find this argument to be persuasive because First Data has produced evidence that various merchants blamed First Data for delays in their compliance status reporting. Accordingly, First Data has provided evidence that there was, indeed, interference with First Data's relationships with third parties.

[23] Maryland law "recognize[s] the doctrine of 'avoidable consequences' in tort actions-the duty to minimize

repudiation of the contract and failure to pay compliance charges provided SecurityMetrics with a right and justifiable cause for its actions.

These theories flounder, however, on the fact that the parties entered the Terms of Settlement. Specifically, the final paragraph of the Terms of Settlement states that the parties "mutually release each other from any and all obligations and claims." As such, SecurityMetrics can no longer rely upon obligations created by the Master Services Agreement and Statement of Work to justify its conduct.[24] Accordingly, SecurityMetrics' Motion for Partial Summary Judgment will be denied with respect to First Data's tortious interference claim.

---

damages-denying recovery of any damages that could have been avoided by reasonable conduct on the part of the plaintiff." *Jones v. Malinowski*, 299 Md. 257, 269 (1984).

[24] Even if this Court were to find that the Terms of Settlement did not operate as such a release, SecurityMetrics' proximate cause argument does not entitle it to summary judgment. Specifically, SecurityMetrics argues that the proximate cause of First Data's alleged damages was not SecurityMetrics' reporting; instead, SecurityMetrics argues that the proximate cause was First Data's repudiation of the contract and its failure to pay for continued START reporting. Thus, rather than alleging that the causal chain was broken, SecurityMetrics has posited that the causal chain reaches back further than First Data claims. Of course, proximate cause is traditionally a question of fact for the jury. *See Lyon v. Campbell*, 120 Md. App. 412, 431-32 (Md. Ct. Spec. App. 1998) ("Tortious conduct may be the proximate cause of an injury without being its sole cause. To create a jury issue, a plaintiff need only introduce evidence to show that, more likely than not, the defendant's wrongful conduct caused the injury alleged. Under this standard of proof, the plaintiff is not required to exclude every possible cause of his injury."(citations omitted)). Because First Data has demonstrated evidence directly linking SecurityMetrics' reporting practices to its claimed damages, this Court finds that summary judgment on the basis of lack of proximate cause is inappropriate.

Similarly, the issue of reducing a damages award based upon the doctrine of avoidable consequences is typically treated as a jury issue. *See, e.g.,* 3 Stein on Personal Injury Damages Treatise § 18:4 (3d ed.) ("[W]hat is a reasonable effort to minimize damages in a given case will depend upon the particular circumstances and is ordinarily a question of fact for the jury.").

Finally, with respect to SecurityMetrics' arguments regarding proof of the elements of a tortious interference claim, SecurityMetrics asserts that First Data has failed to proffer "evidence that SecurityMetrics' conduct is calculated to damage First Data or has an unlawful purpose." This position ignores the undisputed fact that SecurityMetrics still generates START reporting and compliance report spreadsheets for ISOs.

III. First Data's Motion for Summary Judgment as to Certain of SecurityMetrics' Counterclaims (ECF No. 272)

In this motion, First Data moves for summary judgment on SecurityMetrics' fourth through fifteenth counterclaims. These counts include Lanham Act claims, common law torts, and antitrust claims.

A. Lanham Act Counterclaims

1. False Advertising

The Lanham Act prohibits commercial entities from making false statements in their advertising. Specifically, § 43(a)(1)(B) of the Act states that:

> Any person who, on or in connection with any goods or services . . . uses in commerce any . . . false or misleading representation of fact, which . . . , in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

15 U.S.C. § 1125(a)(1)(B). Thus, the Act provides a "private remedy for a commercial plaintiff who meets the burden of proving that its commercial interests have been harmed by a competitor's false advertising." *Made in the USA Foundation v. Phillips Foods, Inc.*, 365 F.3d 278, 281 (4th Cir. 2004) (quoting *Mylan Laboratories, Inc. v. Matkari*, 7 F.3d 1130, 1139 (4th Cir. 1993)). The elements for a false advertising claim under the Lanham Act are:

> (1) the defendant made a false or misleading description of fact or representation of fact in a commercial advertisement about his own or another's product; (2) the misrepresentation is material, in that it is likely to influence the purchasing decision; (3) the misrepresentation actually deceives or has the tendency to deceive a substantial segment of its audience; (4) the

> defendant placed the false or misleading statement in interstate commerce; and (5) the plaintiff has been or is likely to be injured as a result of the misrepresentation, either by direct diversion of sales or by a lessening of goodwill associated with its products.

PBM Products, LLC v. Mead Johnson & Co., 639 F.3d 111, 120 (4th Cir. 2011) (quoting *Scotts Co. v. United Industries*, 315 F.3d 264, 272 (4th Cir. 2002)). With respect to the false or misleading nature of the statement, the advertisement may be "literally false" or an "implied falsehood" that "tend[s] to mislead or confuse consumers." *Id.* (citations omitted). In the case of literal falsehoods, a claimant need not allege nor prove evidence of consumer deception; an implied falsehood, however, requires extrinsic evidence of confusion or deception. *Id.*

SecurityMetrics' false advertising claim address two statements made as part of First Data's promotional materials on its website. The statements at issue are as follows:

> If you choose to use a third-party vendor for PCI DSS compliance services, you will need to contract with and pay that vendor directly. In addition to your alternate vendor's charges for PCI DSS compliance services, you still will need to pay the Compliance Service Fee charged to you by your merchant services provider. The Compliance Service Fee is not affected by your choice to use a third-party vendor.
>
> If First Data's PCI compliance services are contractually available to you, you will be charged an applicable annual compliance fee for those services, regardless of whether you use them or utilize the services of some other third-party PCI compliance services vendor. If you utilize the additional services of a third party vendor, you will pay that third party vendor's charges for those fees in addition to First Data's annual compliance fee.

Countercls. ¶ 112.[25] SecurityMetrics asserts that these statements are actionable under the Lanham Act because First Data actually provides refunds to merchants who use third-party compliance vendors in the amount of the third-party vendor's fee.

In its Motion for Summary Judgment, First Data argues that the statements are literally true and that SecurityMetrics claims essentially that the statements were misleading. First Data argues that such a claim fails because SecurityMetrics has not offered admissible survey evidence demonstrating that the statements were likely to mislead a "substantial segment" of consumers, as required under *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 120 (4th Cir. 2011). In response, SecurityMetrics asserts that it can still prevail on its false advertising counterclaim and avoid summary judgment because, in its view, the statements are literally false and any question regarding the falsity of the statements is an issue of fact to be determined by the jury. *See* SecurityMetrics' Resp. at 7 (citing *C.B. Fleet Co. v. SmithKline Beecham Consumer Healthcare, L.P.*, 131 F.3d 430, 434 (4th Cir. 1997), and *JTH Tax, Inc. v. H & R Block Eastern Tax Servs., Inc.*, 128 F. Supp. 2d 926, 934 (E.D. Va. 2001)).

[25] SecurityMetrics suggests that First Data simply ignored the first statement identified by First Data (and particularly the statement that "[t]he Compliance Service Fee is not affected by your choice to use a third-party vendor."). In its papers, SecurityMetrics argued that First Data's motion should be denied to this first statement because "First Data has not even addressed this other advertisement in its opening brief—and First Data should not be permitted to do so, for the first time, on reply." Reply 6, ECF No. 298. SecurityMetrics reiterated this position at the December 12, 2014 hearing.

Considering that SecurityMetrics presented arguments regarding the first statement, it is clear that SecurityMetrics was aware that First Data's Motion was directed at both statements. Indeed, as First Data points out, First Data's motion cites to both statements, and the statements contain similar content. Considering that First Data had an opportunity to present argument on both statements in both its Response in Opposition *and* at the December 12, 2014 hearing, this Court will not deny First Data's Motion on these grounds.

Thus, the main questions before this Court with respect to the false advertising claim are (1) whether the identified statements are literally true or literally false; and (2) whether the determination of truth or falsity is one that may be decided by this Court on a motion for summary judgment. The first question requires distinguishing between false and misleading statements. The Fourth Circuit has stated that a contested statement "must be either false on its face or, although literally true, likely to mislead and to confuse consumers given the merchandising context." *C.B. Fleet Co. v. SmithKline Beecham Consumer Healthcare, L.P.*, 131 F.3d 430, 434 (4th Cir. 1997). In determining whether an advertisement is literally false, "a court must determine, first, the unambiguous claims made by the advertisement . . . , and second, whether those claims are false." *Scotts Co. v. United Indus. Corp.*, 315 F.3d 264, 274 (4th Cir. 2002) (quoting *Novartis Consumer Health, Inc. v. Johnson & Johnson–Merck Consumer Pharm. Co.*, 290 F.3d 578, 586 (3d Cir. 2002)); *see also id.* ("A literally false message may be either explicit or conveyed by necessary implication when, considering the advertisement in its entirety, the audience would recognize the claim as readily as if it had been explicitly stated." (quoting *Novartis*, 290 F.3d at 586-87)).

Having reviewed the parties' submissions, it is clear that both parties agree that First Data charged its merchants the standard fee but, in some cases, provided a refund in the amount of the third-party vendor's security compliance fee.[26] Merchants were charged the full fee regardless of whether the merchant used a third-party vendor. Thus, when viewed

[26] First Data has further contended that a merchant could receive such a refund only once. *See* Dec. 12, 2014 Hr'g Tr. 35: 1-13.

on their face and in light of the evidence in this case, the statements are not false.[27] The statements are only problematic due to what was left unsaid—that a refund might be available. As such, a reasonable jury could only conclude that the statements are misleading rather than literally false, and, as noted above, such misleading statements require extrinsic evidence of confusion or deception. No such proof is available in this case. Accordingly, First Data is entitled to summary judgment on the false advertising claim.

2. False Endorsement

A claim of false endorsement arises when the name, symbol, or other identifying likeliness is "used in such a way as to deceive the public into believing that [the plaintiff] endorsed, sponsored, or approved of the defendant's product." *Mktg. Products Mgmt., LLC v. Healthandbeautydirect.com, Inc.*, 333 F. Supp. 2d 418, 430 (D. Md. 2004) (quoting *v. Discovery Communications, Inc.*, 200 F.Supp.2d 512, 522 (D. Md. 2002)). Notably, § 43 "goes beyond trademark protection." *Dastar Corp. v. Twentieth Century Fox Film Corp.*, 539 U.S. 23, 28-29 (2003). Specifically, section 43(a)(1)(A) of the Lanham Act, which defines the scope of a false endorsement claim, states that:

> Any person who, on or in connection with any goods or services . . . uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which . . . is likely to cause

[27] Certainly, a case could easily exist where the determination of falsity would require determination by a jury. For example, had SecurityMetrics proffered evidence that First Data *never* charged the compliance fee despite its representations that it would, a jury would need to make factual findings regarding First Data's billing practices and the truth or falsity of its statements in light of those practices. In a case such as this, however, where the facts are not disputed, there is no way that a reasonable jury could conclude that the statement is false on its face rather than simply misleading.

> confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or . . . shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

15 U.S.C. § 1125(a)(1)(A). A false endorsement claim requires proof of the likelihood of consumer confusion as to the original, approval or endorsement of the product or service, which considers "(1) the strength or distinctiveness of the [plaintiff's] mark; (2) the similarity of the two marks; (3) the similarity of the goods and services that the marks identify . . . (6) the defendant's intent; and (7) actual confusion." *Holland v. Psychological Assessment Res, Inc.*, 482 F. Supp. 2d 667, 683 (D. Md. 2007).

SecurityMetrics identifies two bases for its false endorsement claim: (1) the use of the name "PCI Rapid Comply"; and (2) the following statement made by First Data:

> Claims that certain services offered by FDMS are not "approved" by the PCI Security Council or that FDMS is selling PCI compliance products it is not authorized to sell are not true.

Securitymetrics' Resp. at 8 (quoting Countercls. ¶ 119). This Court has already excluded SecurityMetrics' proffered survey evidence regarding consumer perceptions of the name "PCI Rapid Comply." *See* Mem. Op. Mots. *In Limine*, ECF No. 313. This Court sees no basis for permitting that theory to proceed in light of any other evidence in support.[28]

[28] In its Response brief, SecurityMetrics baldly asserts that "First Data's choice of 'PCI Rapid Comply'—not just its inclusion of 'the acronym "PCI"' in that name, but the name as a whole—does indeed falsely imply nonexistent endorsement by the PCI Security Standards Council." SecurityMetrics' Resp. at 7-8. Nothing about the name "PCI Rapid Comply," however, unambiguously implies such endorsement. If anything, the name is ambiguous; as such, SecurityMetrics is required to offer some extrinsic evidence—evidence which it

With respect to the second basis for its claim, SecurityMetrics argues it is entitled to proceed without any survey evidence because the statement is clearly false. *See* Securitymetrics' Resp. at 8 ("The finder of fact needs no survey to conclude that First Data has thereby falsely claimed that its services are approved by the Council and that First Data is authorized to sell those services."). In its reply, First Data argues that this statement is not literally false and, therefore, requires survey evidence. First Data further argues that the terms "approved" and "authorized" are ambiguous and there is no evidence demonstrating that PCI Rapid Comply is not "approved" or "authorized" by the PCI Council, particularly in light of the fact that the service has been operating for two years without any signs of disapproval from the PCI Council. First Data's Reply at 4-5, ECF No. 311.

After reviewing the parties' submissions, this Court concludes that the statement identified by SecurityMetrics is inherently ambiguous. First, the statement references "certain services"—an identification that lacks specificity, although presumably refers to the suite of services offered as part of PCI Rapid Comply. Second, the statement is subject to various interpretations; on the one hand, it suggests that First Data has failed to obtain available certifications, approvals, or authorizations, while on the other hand, it suggests that the services are simply not authorized or approved because such authorizations and approvals are not made by the PCI Council. In light of this ambiguity, the statements cannot be considered literally false; as such, extrinsic evidence is required, and no such

---

has neither produced nor identified.

evidence has been proffered. Accordingly, First Data is entitled to summary judgment on SecurityMetrics' false endorsement claim.

3. Cancellation

SecurityMetrics' Seventh Counterclaim seeks to cancel First Data's registered trademark in "PCI Rapid Comply" pursuant to section 37 of the Lanham Act, 15 U.S.C. § 1119. Here, both parties agree that SecurityMetrics' seventh counterclaim rises or falls with the admissibility of Dr. Belch's survey evidence. First Data's Mem. Supp. Mot. Summ. J. at 16-17, ECF No. 273; SecurityMetrics' Resp. at 8, ECF No. 298. Considering this Court has already ruled that the survey is inadmissible, First Data's Motion for Summary Judgment will be granted with respect to the seventh counterclaim for cancellation.

B. Utah Truth in Advertising Claim

Because it is undisputed that the relevant provisions of the Utah Truth in Advertising Act, Utah Code § 13-11a-3(1)(b), (c), and (e), track the Lanham Act, SecurityMetrics' claims under the state statute fail as well. Accordingly, the First Data's motion will be granted with respect to Count 8 of SecurityMetrics' Counterclaims.

C. Common Law Tort & Damages Claims

SecurityMetrics has asserted two common law tort claims; its fourth counterclaim asserts injurious falsehoods, while its ninth counterclaim asserts tortious interference. In support of its damages claims under these torts, SecurityMetrics has offered evidence in the form of calls and emails in which merchants stated they were canceling or not renewing their contracts with SecurityMetrics.

First Data argues that it is entitled to summary judgment on SecurityMetrics' common law counterclaims for damages because this evidence of allegedly lost customers is inadmissible hearsay evidence.[29] SecurityMetrics argues that these calls are verbal acts because they were instructions to close an account or terminate a contract; therefore, they are not hearsay because they are not offered to prove the truth of any matter asserted.

In *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 565-66 (D. Md. 2007), Judge Grimm provided the basic differentiation between hearsay statements and verbal acts:

> Rule 801(c) states: "Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." (emphasis added). Thus, even if the evidence is an assertion, made by a declarant, it still is not hearsay unless offered to prove the truth of what is asserted. The advisory committee's note to Rule 801(c) underscores this: "If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay. The effect is to exclude from hearsay the entire category of 'verbal acts' and 'verbal parts of an act,' in which the statement itself affects the legal rights of the parties or is a circumstance bearing on conduct affecting their rights." Fed. R. Evid. 801(c) advisory committee's note (citation omitted). *See also* WEINSTEIN at § 801.11[1] ("'If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted.' Thus, if a declarant's statement is not offered for its truth, the declarant's credibility is not material, and the statement is not hearsay." (citation omitted)). Commentators have identified many instances in which assertive statements are not hearsay because they are not offered to prove the truth of the assertions: . . .(4) statements offered as circumstantial evidence of the declarant's

[29] First Data has also argued that (1) the request for damages was not properly pled; (2) SecurityMetrics never timely supplied a calculation of its damages to First Data; and (3) the claimed damages are not causally tied to First Data's alleged conduct.

> state of mind, or motive; (5) statements that have relevance simply because they were made, regardless of their literal truth or falsity-the so called "verbal acts or parts of acts," also referred to as "legally operative facts"; and (6) statements that are questions or imperative commands, such as "what time is it" or "close the door."

Id. (footnotes omitted). Assuming *arguendo* that the various statements concerning cancellation and/or renewal in the calls and emails qualify as verbal acts, there is still a further hearsay problem. While the statements concerning the cancellation or non-renewal may be admissible, those statements do not wholly satisfy SecurityMetrics' burden of proof. Those statements, taken alone, provide no link between First Data's alleged actions and the cancellation or non-renewal by those particular merchants. Thus, it is the other statements made in those calls and emails that SecurityMetrics seeks to use as evidence of causation.

However, SecurityMetrics alternatively offers the calls and emails as evidence of the customers' intent to terminate or not renew "or to show *why*" they acted or decided as they did under Rule 803(3) of the Federal Rules of Evidence. Specifically, Rule 803(3) states:

> A statement of the declarant's then-existing state of mind (such as motive, intent, or plan) or emotional, sensory, or physical condition (such as mental feeling, pain, or bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the validity or terms of the declarant's will.

F.R.E. 803(3). First Data harps upon SecurityMetrics' characterization of the statement as evidence showing "why" the merchants did, decided, or intended as they did; First Data argues that "why" someone had a particular state of mind constitutes a statement of memory

or belief expressly excluded by Rule 803(3) because it is offered to prove the fact remembered or believed.

This Court finds the reasoning of *Air Turbine Tech., Inc. v. Atlas Copco AB*, 295 F. Supp. 2d 1334, 1345-46 (S.D. Fla. 2003), *aff'd*, 410 F.3d 701 (Fed. Cir. 2005), persuasive. In that case, the district court granted summary judgment after it ruled that customer statements regarding the reasons for their dissatisfaction were inadmissible hearsay when offered to prove causation with respect to lost customers. Moreover, just as in that case, SecurityMetrics has failed to obtain such evidence directly from customers and has opted to instead rely solely on the recorded phone calls and emails. As these materials are the only evidence offered to demonstrate causation of damages, SecurityMetrics has failed to offer any admissible evidence in support of its common law counterclaims. Accordingly, First Data's motion will be granted with respect to counts four and nine of SecurityMetrics' counterclaims.

D. Antitrust Counterclaims

Counts ten through fifteen of SecurityMetrics' counterclaims assert various antitrust claims under federal and Maryland law. SecurityMetrics includes a number of different theories of liability in its counterclaims, including a tying claim and an attempted monopolization claim.

The antitrust laws "are intended to protect competition, and not simply competitors"; accordingly, "only injury caused by damage to the competitive process may form the basis

for an antitrust claim" by a private person." *Thompson Everett, Inc. v. Nat'l Cable Advert.*, 57 F.3d 1317, 1325 (4th Cir. 1995). Thus, "to be recovered as antitrust damages, a competitor's loss of profits must stem from a competition-reducing aspect or effect of the defendant's behavior, that is, from acts that reduce output or raise prices to consumers." *Continental Airlines, Inc. v. United Airlines, Inc.*, 277 F.3d 499, 515-16 (4th Cir. 2002) (internal citations, alterations, and quotation marks omitted).

First Data argues that SecurityMetrics' antitrust counterclaims fail because SecurityMetrics has failed to demonstrate injury to competition rather than simply injury to SecurityMetrics; specifically, First Data asserts that SecurityMetrics "has never alleged, and cannot prove, that First Data had any adverse effect on the availability, prices, quantity, quality, or competitive landscape of PCI reporting/validation services or has otherwise cause any harm to competition." Mem. Supp. Mot. Summ. J. Certain Countercls. 26, ECF No. 272. First Data also argues that the concept of harm to competition requires expert analysis and that SecurityMetrics has simply failed to obtain any such testimony. *See id.* at 27-28.

In response, SecurityMetrics argues that there is evidence of injury to competition because First Data's conduct has reduced output and frustrated price competition.

With respect to reduced output, SecurityMetrics asserts that it lost over 280,000 merchant customers and that approximately 210,000 of those merchants no longer appear to have a PCI validation and compliance vendor. In SecurityMetrics' view, this constitutes a reduction of output; specifically, SecurityMetrics alleges that First Data has directly profited from this development because First Data can assess Non-receipt of PCI Validation Fees,

which SecurityMetrics alleges is First Data's biggest PCI compliance revenue opportunity. SecurityMetrics' Resp. at 31.

In its Reply, First Data preliminarily argues that SecurityMetrics only proposed its reduced output theory for the first time at the summary judgment stage and that, as such, the claim should be rejected. Reply at 15 (citing *Harris v. Reston Hosp. Ctr., LLC*, 553 F. App'x 938, 947 (4th Cir. April 24, 2013) (unpublished), for the proposition that new theories are prohibited at the summary judgment stage). Indeed, this Court has been unable to identify any discussion of such a theory anywhere else in the docket.

Even if SecurityMetrics had properly raised the issue of reduced output, this Court does not find that SecurityMetrics' allegations are sufficient to survive First Data's motion for summary judgment. No expert has testified to the issue of reduced output, and SecurityMetrics reference to merchants who have dropped off the PCI compliance service rolls is purely speculative. Without conducting any third-party discovery, SecurityMetrics simply assumes that those merchants have continued operations without obtaining a new compliance services vendor. Moreover, SecurityMetrics has provided no analysis to back up its assertions regarding the profitably and revenue potential from First Data's non-compliance fees. SecurityMetrics' reduced output theory—suddenly posited and utterly devoid of factual development in support—is insufficient to warrant a finding of injury to competition in this case.

With respect to harm to price competition, SecurityMetrics alleges that:

> The mass migration from SecurityMetrics to First Data

> shows that price competition has been impaired. As of June 1, 2012, SecurityMetrics' pricing direct to merchants ranged between $29.99 and $139.99 per year; over the next couple months, SecurityMetrics contracted that range to between $49.99 and $99.99. (Ex. I at 97:8–102:16.) SecurityMetrics' pricing to ISOs ranges between $1.75 and $2.50 per merchant per month. (Ex. at ¶ 6.) First Data's direct-to-merchants pricing, by contrast, has ranged from $79.00 to $124.99 per year and its ISO pricing is $3 per merchant per month. (*See* Mem. at 10, 31.) But still First Data is gaining and SecurityMetrics is losing . . . .

SecurityMetrics' Resp. at 33, ECF No. 298 (footnote omitted). SecurityMetrics alleges that it and the third and fourth largest providers compete against each other in price but that First Data, as the largest provider with 300,000 merchants, does not.

First Data further asserts that SecurityMetrics has failed to offer any expert testimony in support of its assertions. Indeed, this Court is troubled that SecurityMetrics intends to proceed on such a claim absent any expert testimony. SecurityMetrics looks only to the prices of First Data and itself and includes no factual discussion or analysis of the price of competitors in the market place.[30] In light of these circumstances, this Court has no choice but to find that SecurityMetrics has failed to offer sufficient evidence to survive First Data's Motion for Summary Judgment with respect to the antitrust counterclaims.[31]

---

[30] The only piece of evidence that SecurityMetrics identifies is the Declaration of Bradley Caldwell, in which Mr. Caldwell states that, with respect to SecurityMetrics' pricing, "[m]ost commonly the price term is negotiated to about $2 per merchant, to compete with non-FDMS or third party providers such as Trustwave." *See* SecurityMetrics' Resp. at Ex. C. ¶ 6, ECF No. 298-3.

[31] In finding that SecurityMetrics has failed to demonstrate any injury to competition that is actionable under the antitrust laws, this Court makes no ruling on the various other arguments raised by First Data with respect to the specific antitrust claims and theories. Nevertheless, the Court notes that it is troubled by SecurityMetrics' attempted monopolization counterclaims; SecurityMetrics lacks any expert testimony to support its claim and it essentially seeks to disguise a variety of alleged business torts and Lanham Act violations as antitrust violations. *See* SecurityMetrics' Resp. at 27 ("The factual predicates for SecurityMetrics'

IV. Other Outstanding Matters

By letter dated December 10, 2014 (ECF No. 321), SecurityMetrics requested clarification regarding this Court's December 3, 2014 Memorandum Opinion and accompanying Order on First Data's motions *in limine*. Additionally, SecurityMetrics indicated that it would seek to file a formal motion for reconsideration if this Court's ruling was intended to exclude its phone call recording and email evidence in addition to the charts submitted as part of Dr. Nelson's expert report. The parties' papers on the motions for summary judgment were filed before this Court's ruling on the motions *in limine*, and this Court considered all such evidence in its consideration of the motions for summary judgment. Because this Court finds that SecurityMetrics' counterclaims fail even if this

---

attempted monopolization include (1) all those on which its other antitrust claims are based, (2) the defamation campaign discussed above in connection with SecurityMetrics' injurious falsehood claim, (3) the false advertising and endorsement claims discussed above in connection with SecurityMetrics' Lanham Act claims, (4) First Data's reckless instigation of a series of disingenuous legal proceedings having as their apparent object driving SecurityMetrics (First Data's only serious competitor for the 820,000 merchants at issue) from the field, and (5) First Data's ACF and associated refund policies. By that conduct, First Data has attempted to monopolize the market for PCI compliance services provided to the 820,000 merchants to which it provides both transaction processing and what it calls "acquirer services," in violation of Section 2 of the Sherman Act, 15 U.S.C. § 2, and Maryland Commercial Law Code § 11-204(a)(2)."). The Fourth Circuit has noted that such bootstrapping attempts warrant suspicion from the courts. *See Military Servs. Realty, Inc. v. Realty Consultants of Virginia, LTD*, 823 F.2d 829, 832 n.4 (4th Cir. 1987) ("[C]ourts should be circumspect in converting ordinary business torts into violations of antitrust laws. To do so would be to create a federal common law of unfair competition which was not the intent of the antitrust laws." (quoting *Merkle Press, Inc. v. Merkle*, 519 F. Supp. 50 (D. Md. 1981)). Such suspicion is certainly warranted in this case because First Data is already winding down the PCI Rapid Comply program, which was the primary basis of SecurityMetrics' other antitrust claims.

Further complicating SecurityMetrics' attempt to recover its lost profits is the fact that SecurityMetrics' damages expert (Dr. Nelson) failed to disaggregate his damages calculations. Thus, failure on one of its counterclaims—or simply one of the theories posited in any of those various counterclaims—would give rise to serious issues regarding Dr. Nelson's calculations. *See* Mem. Op. Mots. *In Limine* at 24 n.27, ECF No. 313 (noting that failure to disaggregate calculation of damages based upon claims becomes problematic after one or more theories of liability are eliminated from a case); *see also Pharmanetics, Inc. v. Aventis Pharmaceuticals, Inc.*, 182 F. App'x 267 (4th Cir. May 31, 2006) (unpublished); *Comcast Corp. v. Behrend*, --- U.S. ----, 133 S. Ct. 1426 (2013).

Court were to grant reconsideration, SecurityMetrics' request is DENIED AS MOOT.

There are also several other substantive motions that remain pending on the docket. First Data's Motion to Strike the November 12, 2014 'Pinch-Hitting' Declaration of Expert Robert J. Philbin (ECF No. 310) was denied for the reasons indicated on the record at the December 12, 2014 hearing. SecurityMetrics' Motion *in Limine* to Exclude Portions of Expert Report and Testimony of J. Gregory Sidak (ECF No. 296) is DENIED AS MOOT because First Data's has prevailed on its motion for summary judgment with respect to SecurityMetrics' antitrust counterclaims. Finally, the parties have alerted the Court to a troubling situation regarding the credentials of Richard Gering, one of First Data's rebuttal experts. Specifically, it appears that Mr. Gering does not have a Ph.D., as he represented in his expert report and testimony. The Court held a conference call to address this issue on December 22, 2014; during that call, First Data indicated that it would not (and could not) put Mr. Gering on the stand. According, SecurityMetrics' Motion *in Limine* to Exclude Portions of Dr. Richard Gering's Report, Testimony, and Demonstrative Exhibits (ECF No. 300) will be GRANTED AS MOOT. First Data has also sought to substitute a new expert witness for Mr. Gering, and that request has been denied on this date by a separate Letter Order.

CONCLUSION

For the reasons stated above, First Data's Motion for Summary Judgment as to Certain of SecurityMetrics' Counterclaims (ECF No. 272) is GRANTED. SecurityMetrics' Motion for Partial Summary Judgment on Contract Claims and Counterclaims (ECF No.

275) is DENIED and First Data's Cross-Motion for Summary Judgment as to First Counterclaim (ECF No. 294) is GRANTED. Additionally, SecurityMetrics' Motion for Partial Summary Judgment on Common Law Tort and Lanham Act Claims (Counts III-VIII) (ECF No. 277) is DENIED AS MOOT with respect to First Data's Lanham Act claims and DENIED with respect to First Data's tortious interference claim.

The Court also makes the following evidentiary rulings. SecurityMetrics' request for clarification and/or reconsideration (ECF No. 321) is DENIED AS MOOT. First Data's Motion to Strike the November 12, 2014 'Pinch-Hitting' Declaration of Expert Robert J. Philbin (ECF No. 310) was denied for the reasons indicated on the record at the December 12, 2014 hearing. SecurityMetrics' Motion *in Limine* to Exclude Portions of Expert Report and Testimony of J. Gregory Sidak (ECF No. 296) is DENIED AS MOOT. SecurityMetrics' Motion *in Limine* to Exclude Portions of Dr. Richard Gering's Report, Testimony, and Demonstrative Exhibits (ECF No. 300) is GRANTED AS MOOT.

Accordingly, this matter is now ready to proceed to trial. With respect to First Data's claims, the following counts remain: declaratory relief (Counts 1 & 9), breach of contract (Count 2), and tortious interference (Count 4). With respect to SecurityMetrics' counterclaims, the following counts remain: declaratory judgment with respect to the third paragraph of the Terms of Settlement (Count 2), and declaratory judgment with respect to the fifth paragraph of the Terms of Settlement (Count 3).

A separate Order follows.

Dated: December 30, 2014

/s/
Richard D. Bennett
United States District Judge